ASYMPTOTIC OF NUMBER OF SIMILARITY CLASSES OF COMMUTING TUPLES

UDAY BHASKAR SHARMA

Abstract. Let $c(n,k,q)$ be the number of simultaneous similarity classes of k-tuples of commuting $n \times n$ matrices over a finite field of order q. We show that, for a fixed n and q, $c(n,k,q)$ is asymptotically $q^{m(n)k}$ (upto some constant factor), as a function of k, where $m(n) = [n^2/4]+1$ is the maximal dimension of a commutative subalgebra of the algebra of $n \times n$ matrices over the finite field.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of order q, n be a positive integer, $M_n(\mathbb{F}_q)$ be the algebra of $n \times n$ matrices over $\mathbb{F}_q$, and $GL_n(\mathbb{F}_q)$, the group of invertible $n \times n$ matrices. Then, by the theory of the rational canonical form, the number of similarity classes in $M_n(\mathbb{F}_q)$ is given by

$$c(n,1,q) = \sum_{\lambda \vdash n} q^{\lambda_1},$$

where λ varies over partitions of n, and each λ is of the form:

$$\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots).$$

It can clearly be seen that, keeping n fixed, $c(n,k,q)$ as a function of q is asymptotically q^n upto multiplication by some constant factor. If we keep q fixed and look at $c(n,1,q)$ as a function of n, then also, it is asymptotically q^n upto multiplication by a constant. This is a non-trivial asymptotic result, which Stong [Sto88] proved in 1988. In 1995, Neumann and Praeger [NP95] looked at the probability of an $n \times n$ matrix over $\mathbb{F}_q$ being non-cyclic and found that, for a fixed q, the probability of a $n \times n$ matrix over $\mathbb{F}_q$ being non-cyclic, is asymptotically q^{-3} as a function of n. They also looked at non-separable matrices, and proved that the probability of a matrix in $M_n(\mathbb{F}_q)$ being non-separable is asymptotically q^{-1}, upto multiplication by a constant.

Date: May 30, 2016.
2010 *Mathematics Subject Classification.* 05A16.
Key words and phrases. Matrices over finite fields, Asymptotic, Similarity classes, Commuting tuples of matrices.

In 1998, Girth [Gir98] worked on certain probabilities for $n \times n$ upper triangular matrices and compared their asymptotic behaviour with that of corresponding probabilities for arbitrary $n \times n$ matrices over $\mathbb{F}_q$. He also did these comparisons of asymptotic behaviours as q goes to ∞, keeping n fixed. The works mentioned above focus mainly on counting in $M_n(\mathbb{F}_q)$ and finding the asymptotic behaviours as n goes to ∞.

In this paper, we shall consider for any positive integer k, the space $M_n(\mathbb{F}_q)^k$ of k-tuples of $n\times n$ matrices over $\mathbb{F}_q$. $GL_n(\mathbb{F}_q)$ acts on $M_n(\mathbb{F}_q)^k$ by simultaneous conjugation, which is defined as follows:

$$\text{For } g \in GL_n(\mathbb{F}_q), \text{ and } (A_1, \ldots, A_k) \in M_n(\mathbb{F}_q)^k,$$

$$g.(A_1, \ldots, A_k) = (gA_1g^{-1}, gA_2g^{-1}, \ldots, gA_kg^{-1}).$$

The orbits for this action are called *simultaneous similarity classes*.

Let $a(n, k, q)$ denote the number of simultaneous similarity classes in $M_n(\mathbb{F}_q)^k$. Then, by Burnside's lemma we have,

$$a(n, k, q) = \frac{1}{|GL_n(\mathbb{F}_q)|} \sum_{g \in GL_n(\mathbb{F}_q)} |Z_{M_n(\mathbb{F}_q)}(g)|^k,$$

where for each $g \in GL_n(\mathbb{F}_q)$, $Z_{M_n(\mathbb{F}_q)}(g)$ denotes the centralizer algebra of g i.e.,

$$Z_{M_n(\mathbb{F}_q)}(g) = \{x \in M_n(\mathbb{F}_q) \mid xg = gx\}.$$

Claim 1. *We claim that, keeping n and q fixed, $a(n, k, q)$ is asymptotically q^{n^2k} up to some constant factor, as k goes to ∞.*

Proof. We need to show that there exist positive constants, m_1 and m_2 (constant with respect to k), such that: $m_1q^{n^2k} \leq a(n, k, q) \leq m_2q^{n^2k}$. So, in the Burnside lemma expansion of $a(n, k, q)$, just consider all those g that are scalar matrices. Then, we have $Z_{M_n(\mathbb{F}_q)}(g) = M_n(\mathbb{F}_q)$. So, taking m_1 to be

$$m_1 = \frac{q - 1}{|GL_n(\mathbb{F}_q)|},$$

we have $m_1q^{n^2k} \leq a(n, k, q)$.

Next, if g is a non-scalar matrix, then $Z_{M_n(\mathbb{F}_q)}(g) \subsetneq M_n(\mathbb{F}_q)$. We know (see Agore [Ago14]), that the maximal dimension of a proper subalgebra of $M_n(\mathbb{F}_q)$ is, $n^2 - n + 1$.

So we have

$$\begin{aligned} a(n,k,q) &= \frac{1}{|GL_n(\mathbb{F}_q)|} \sum_{g \in GL_n(\mathbb{F}_q)} |Z_{M_n(\mathbb{F}_q)}(g)|^k \\ &= \frac{1}{|GL_n(\mathbb{F}_q)|}(q-1)q^{n^2k} + \sum_{\substack{g \in GL_n(\mathbb{F}_q) \\ g \notin \mathbb{F}_q.I_n}} |Z_{M_n(\mathbb{F}_q)}(g)|^k \\ &\leq \frac{1}{|GL_n(\mathbb{F}_q)|}(q-1)q^{n^2k} + \sum_{\substack{g \in GL_n(\mathbb{F}_q) \\ g \notin \mathbb{F}_q.I_n}} q^{(n^2-n+1)k} \\ &= \frac{1}{|GL_n(\mathbb{F}_q)|}(q-1)q^{n^2}k \left(1 + (|GL_n(\mathbb{F}_q)| - q + 1)q^{-(n-1)k}\right). \end{aligned}$$

From this, we get m_2 such that $a(n,k,q) \leq m_2 q^{n^2k}$. Thus the claim is proved. $\square$

Now, denote by $M_n(\mathbb{F}_q)^{(k)}$, the set of k-tuples of commuting matrices from $M_n(\mathbb{F}_q)$, i.e., the set,

$$M_n(\mathbb{F}_q)^{(k)} = \{(A_1, \ldots, A_k) \in M_n(\mathbb{F}_q)^k \mid A_iA_j = A_jA_i \text{ for } i \neq j\}.$$

Let $c(n,k,q)$ denote the number of simultaneous similarity classes in $M_n(\mathbb{F}_q)^{(k)}$ under the simultaneous conjugation by $GL_n(\mathbb{F}_q)$ on it. The aim of the paper is to find for a fixed n and q, an asymptotic for $c(n,k,q)$ as a function of k. The problem here is that, the technique used in the proof of Claim 1 fails in this case because the matrices, $A_1, ..., A_k$, are no longer independently chosen.

In [Sha16], $c(n,k,q)$ was calculated for $n = 2, 3, 4$. The leading terms of some of those values are shown in Table 1.

From Table 1, we see that $c(2,k,q)$ is asymptotically q^{2k}. $c(3,k,q)$ is asymptotically q^{3k} and $c(4,k,q)$ is asymptotically $q^{5k-7} = q^{-7}q^{5k}$. In the case of $n = 4$, we see that $c(4,k,q)$ is asymptotically q^{5k} (and not q^{4k}, as we would expect), up to a constant factor which is q^{-7}.

The number 5 is the maximal dimension for any commutative subalgebra of $M_4(\mathbb{F}_q)$. In fact, Jacobson [Jac44] showed that, for any positive integer n, the maximal dimension of any commutative subalgebra of $M_n(\mathbb{F}_q)$ is

$$m(n) = \left[\frac{n^2}{4}\right] + 1.$$

k	$c(2,k,q)$	$c(3,k,q)$	$c(4,k,q)$
1	q^2+q	q^3+q^2+q	$q^4+q^3+2q^2+2$
2	$q^4+q^3+q^2$	$q^6+q^5+2q^4+\cdots$	$q^8+q^7+\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
7	$q^{14}+q^{13}+\cdots$	$q^{21}+q^{20}+\cdots$	$2q^{28}+q^{27}+\cdots$
8	$q^{16}+q^{15}+\cdots$	$q^{24}+q^{23}+\cdots$	$q^{33}+q^{32}+\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
20	$q^{40}+q^{39}+\cdots$	$q^{60}+q^{59}+\cdots$	$q^{93}+q^{92}+\cdots$
21	$q^{42}+q^{41}+\cdots$	$q^{63}+q^{62}+\cdots$	$q^{98}+q^{97}+\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

TABLE 1. Leading terms of $c(n,k,q)$ for $n = 2,3,4$

Coming back to $n = 2,3,4$, we see that $m(2) = 2$, $m(3) = 3$ and $m(4) = 5$. So for $n \in \{2,3,4\}$, $c(n,k,q)$ is asymptotically $q^{m(n)k}$ up to some constant factor. We claim this is true for any n. Thus we have the main theorem of this paper:

Theorem 1.1. *For a fixed positive integer n and prime power q, $c(n,k,q)$ as a function of k, is asymptotic to $q^{m(n)k}$ up to some constant factor.*

1.1. **Outline of the Paper.** In Section 2, we will prove the main theorem (Theorem 1.1). In Section 3, we will find out the asymptotic of counting the total number of k-tuples of commuting matrices over $\mathbb{F}_q$ i.e., the cardinality of $M_n(\mathbb{F}_q)^{(k)}$.

2. Proof of Theorem 1.1

To prove Theorem 1.1, it suffices to prove the existence of positive numbers, C_1 and C_2, such that:

$$C_1 q^{m(n)k} \leq c(n,k,q) \leq C_2 q^{m(n)k}$$

for large k. Before we go ahead, we will need to unravel $c(n,k,q)$.

We first define the following:

Definition 2.1. *Let $Z \subseteq M_n(\mathbb{F}_q)$ be a subalgebra, and Z^* be the group of units of Z. For positive integer k, let $c(Z,k,q)$ denote the number of simultaneous similarity classes of k-tuples of commuting matrices in Z, under the conjugation action by Z^*.*

For $k = 0$ and any subalgebra $Z \subseteq M_n(\mathbb{F}_q)$, $c(Z, 0, q) = 1$.

We claim:

$$c(n,k,q) = \sum_{Z \subseteq M_n(\mathbb{F}_q)} c_Z c(Z, k-1, q), \tag{2.1}$$

where Z runs over subalgebras of $M_n(\mathbb{F}_q)$, c_Z is the number of similarity classes in $M_n(\mathbb{F}_q)$, whose centralizer algebra is conjugate to Z.

Let $(A_1, \dots, A_k) \in M_n(\mathbb{F}_q)^{(k)}$. Let $Z = Z_{M_n(\mathbb{F}_q)}(A_1)$. Then it is clear that $(A_2, \dots, A_k) \in Z^{(k-1)}$. The map,

$$(A_1, \dots, A_k) \mapsto (A_2, \dots, A_k),$$

induces a bijection between the set of simultaneous similarity classes in $M_n(\mathbb{F}_q)^{(k)}$, which have an element whose first coordinate is A_1, and the orbits for the simultaneous conjugation action of Z^* on $Z^{(k-1)}$. Hence we get the identity (2.1).

Now, in identity (2.1), for each Z, we can expand $c(Z, k-1, q)$ (when $K \geq 2$) to get

$$c(Z, k-1, q) = \sum_{Z' \subseteq Z} c_{ZZ'} c(Z', k-2, q),$$

where $c_{ZZ'}$ is the number of orbits of matrices in Z for the action of Z^* on it by conjugation, whose centralizer algebra under this conjugation action is conjugate to Z'.

Proceeding this way, we get the following expansion for $c(n,k,q)$:

$$c(n,k,q) = \sum_{Z_1 \supseteq \cdots \supseteq Z_k} c_{Z_1} c_{Z_1 Z_2} \cdots c_{Z_{k-1} Z_k}, \tag{2.2}$$

where, for $1 \leq i \leq k-1$, Z_i is the common centralizer of some i-tuple of commuting matrices $(A_1, \dots, A_i)$, i.e.,

$$Z_i = \bigcap_{j=1}^{i} Z_{M_n(\mathbb{F}_q)}(A_j),$$

and $c_{Z_i Z_{i+1}}$ denotes the number of orbits of matrices in Z_i for the conjugation action of Z_i^*, whose centralizer algebra in Z_i, is conjugate to Z_{i+1}. For $Z_{i+1} \subseteq Z_i$, we say that Z_{i+1} is a **branch** of Z_i, if $c_{Z_i Z_{i+1}} > 0$.

Here are some observations about these non-increasing sequences of subalgebras which come up in the expansion of $c(n,k,q)$. We shall state them as a lemma:

Lemma 2.2. *Given a non-increasing sequence of centralizer subalgebras which occurs in equation (2.2), say*

$$Z_1 \supseteq \cdots \supseteq Z_k,$$

we have the following:

(1) *If for some i, Z_i is a commutative subalgebra, then*

$$Z_{i+1} = \cdots = Z_k = Z_i$$

and for each j $(i \leq j \leq k-1)$,

$$c_{Z_j Z_{j+1}} = q^{\dim(Z_i)}.$$

(2) *If Z_i is not necessarily commutative, but if $Z_{i+1} = Z_i$, then*

$$c_{Z_i Z_{i+1}} = q^{\dim(Z(Z_i))},$$

where $Z(Z_i)$ is the centre of Z_i.

Proof. For $i \geq 1$, let $(A_1, \ldots, A_i) \in M_n(\mathbb{F}_q)^{(k)}$, such that

$$Z_i = \bigcap_{j=1}^{i} Z_{M_n(\mathbb{F}_q)}(A_j).$$

(1) Suppose, for some i, Z_i is commutative. Then, for any element, $A_{i+1} \in Z_i$, its centralizer $Z_{Z_i}(A_{i+1})$ in Z_i, is Z_i itself. Therefore, we have

$$Z_{i+1} = \bigcap_{j=1}^{i+1} Z_{M_n(\mathbb{F}_q)}(A_j) = Z_{Z_i}(A_{i+1}) = Z_i,$$

and therefore $c_{Z_i Z_{i+1}} = |Z_i| = q^{\dim(Z_i)}$. Similarly, $Z_j = Z_i$ for $i+1 \leq j \leq k$. Thus, $c_{Z_j Z_{j+1}} = q^{\dim(Z_i)} \leq q^{m(n)}$ for $i \leq j \leq k-1$.

(2) If Z_i is not necessarily commutative but, $Z_{i+1} = Z_i$, then $c_{Z_i Z_{i+1}}$ is the number of matrices A_{i+1} in Z_i for which

$$Z_{Z_i}(A_{i+1}) = Z_i.$$

Thus $c_{Z_i Z_{i+1}}$ is the size of the centre $Z(Z_i)$, of Z_i. So

$$c_{Z_i Z_{i+1}} = q^{\dim(Z(Z_i))} \leq q^{m(n)}.$$

$\square$

2.1. **Finding Crude Lower and Upper bounds for $c(n,k,q)$.** The first and main thing we need to show is that there exists a tuple of commuting matrices whose common centralizer is a commutative algebra of dimension $m(n)$. Here are examples of tuples of commuting matrices whose common centralizer is a commutative subalgebra of $M_n(\mathbb{F}_q)$ of dimension $m(n)$.

Example 2.3. *When n is even, say $n = 2l$, for some $l \geq 1$, we have*

$$m(n) = l^2 + 1.$$

Consider the commuting tuple, $(A_1, A_2, \ldots, A_{l+1})$, in which

$$A_1 = \begin{pmatrix} 0_l & I_l \\ 0_l & 0_l \end{pmatrix},$$

where 0_l is the $l \times l$ 0-block, and I_l is the $l \times l$ identity matrix. For $i \geq 2$,

$$A_i = \begin{pmatrix} 0_l & N_i \\ 0_l & 0_l \end{pmatrix},$$

where for $i = 2, \ldots, l+1$,

$$N_i = \begin{pmatrix} 0_{(l-1)\times l} \\ e_{i-1} \end{pmatrix} \ \text{($0_{(l-1)\times l}$ is the $(l-1)\times l$ 0-block)}$$

and e_{i-1} is the $1 \times l$ row matrix

$$\begin{pmatrix} 0 \cdots & \underset{(i-1)th\ place}{\overset{1}{\downarrow}} & \cdots 0 \end{pmatrix}.$$

Its common centralizer algebra is

$$Z = \left\{ a_0 I_n + \begin{pmatrix} 0_l & B \\ 0_l & 0_l \end{pmatrix} \ : a_0 \in \mathbb{F}_q \text{ and } B \in M_l(\mathbb{F}_q) \right\}.$$

It is commutative and is of dimension $l^2 + 1$.

Example 2.4. *When n is odd, say $n = 2l + 1$ for some $l \geq 1$, then $m(n) = l(l+1) + 1$. Consider the commuting tuple $(A_1, A_2, \ldots, A_{l+1})$ where*

$$A_1 = \begin{pmatrix} 0_{(l+1)\times(l+1)} & I_l \\ 0_{l\times(l+1)} & 0_{(l+1)\times l} \end{pmatrix},$$

and for $i = 2, \ldots, l+1$,

$$A_i = \begin{pmatrix} 0_{(l+1)\times(l+1)} & N_i \\ 0_{l\times(l+1)} & 0_{l\times l} \end{pmatrix},$$

where for each i, N_i is a $(l+1) \times l$-matrix of the form

$$\begin{pmatrix} 0_{l\times l} \\ e_{i-1} \end{pmatrix},$$

where e_{i-1} is as defined in Example 2.3. Then the common centralizer of this tuple of commuting matrices is

$$\left\{ a_0 I_n + \begin{pmatrix} 0_{(l+1)\times(l+1)} & B \\ 0_{l\times(l+1)} & 0_{l\times l} \end{pmatrix} : a_0 \in \mathbb{F}_q \text{ and } B \in M_{(l+1)\times l}(\mathbb{F}_q) \right\}.$$

It is commutative and is of dimension $l(l+1)+1$, which is equal to $m(n)$.

So we can find at least a $([n/2]+1)$-tuple of commuting $n\times n$ matrices, whose common centralizer algebra is of dimension $m(n)$.

Lemma 2.5. *There exists $C_1 > 0$ such that $C_1 q^{m(n)k} \leq c(n,k,q)$ for large k.*

Proof. Let $l_0 = \left[\frac{n}{2}\right] + 1$. Consider the k-tuple,

$$(A_1, A_2, \ldots, A_{l_0}, A_{l_0+1}, \ldots, A_k),$$

where the first l_0 matrices of the commuting tuple are as in Examples 2.3 or 2.4 (depending on whether n is even or odd). Here, Z_{l_0} is a commutative subalgebra of dimension $m(n)$ (as described in the examples). Hence, by Lemma 2.2, for $i = l_0+1, \ldots, k$, $Z_i = Z_{l_0}$. Then

$$c(n,k,q) \geq c_{Z_1} c_{Z_1 Z_2} \cdots c_{Z_{l_0-1} Z_{l_0}} q^{m(n)(k-l_0)}.$$

Let

$$C_1 = \frac{c_{Z_1} c_{Z_1 Z_2} \cdots c_{Z_{l_0-1} Z_{l_0}}}{q^{m(n) l_0}}$$

then $c(n,k,q) \geq C_1 q^{m(n)k}$ for all large k.

□

To complete the proof of the Theorem 1.1, we need the following observation (Lemma 2.6), about the non-increasing sequences of subalgebras, $Z_1 \supseteq \cdots \supseteq Z_k$, which occur in the expansion of $c(n,k,q)$ (given in equation (2.2)).

Lemma 2.6. *$Z(Z_i) \subseteq Z(Z_{i+1})$ for $i \geq 1$ and if $Z_{i+1} \subsetneq Z_i$, then $Z(Z_i) \subsetneq Z(Z_{i+1})$*

Proof. Let $x \in Z(Z_i)$. Then, for any $y \in Z_i$ such that $Z_{Z_i}(y) = Z_{i+1}$, $xy = yx$ implies that $x \in Z_{i+1}$. Now, as $x \in Z(Z_i)$, $xz = zx$ for every $z \in Z_{i+1}$, which implies that, $x \in Z(Z_{i+1})$. So $Z(Z_i) \subseteq Z(Z_{i+1})$ and thus $\dim(Z(Z_{i+1})) \geq \dim(Z(Z_i))$.

If $Z_i \supsetneq Z_{i+1}$. Then consider any $y \in Z_i$ for which $Z_{Z_i}(y) = Z_{i+1}$. Clearly, $y \in Z(Z_{i+1})$. But, for $x \notin Z_{i+1}$, $yx \neq xy$. Hence $y \notin Z(Z_i)$. Therefore $Z(Z_i) \subsetneq Z(Z_{i+1})$. Thus $\dim(Z(Z_{i+1})) > \dim(Z(Z_i))$. □

Now we are in a position to get a crude upper bound for $c(n,k,q)$. Let $k > n^2$. Let us look at any summand of $c(n,k,q)$. A summand of $c(n,k,q)$ is of the form,

$$c_{Z_1}c_{Z_1Z_2}\cdots c_{Z_{k-1}Z_k},$$

where $Z_1 \supseteq Z_2 \supseteq \cdots \supseteq Z_k$. Let j be the number of distinct Z_i's in the non-increasing sequence. As $M_n(\mathbb{F}_q)$ is of dimension n^2, there cannot be more than n^2 distinct Z_i's in this non-increasing sequence, $Z_1 \supseteq Z_2 \supseteq \cdots \supseteq Z_k$, of subalgebras of $M_n(\mathbb{F}_q)$. So $1 \le j \le n^2$.

We therefore rewrite $c(n,k,q)$ as

$$c(n,k,q) = \sum_{j=0}^{n^2-1} \sum_{\substack{Z_1\supseteq\cdots\supseteq Z_k \\ j+1 \text{ distinct}}} c_{Z_1}c_{Z_1Z_2}\cdots c_{Z_{k-1}Z_k} \tag{2.3}$$

Now, for any $j:\ 0 \le j \le n^2-1$; consider a non-increasing sequence, $Z_1 \supseteq \cdots \supseteq Z_k$, in which $j+1$ of the Z_i's are distinct. Then it has a strictly decreasing subsequence,

$$Z_{i_1} \supsetneq Z_{i_2} \supsetneq \cdots \supsetneq Z_{i_j} \supsetneq Z_k.$$

So the non-increasing sequence, $Z_1 \supseteq \cdots \supseteq Z_k$, looks like this:

$$Z_1 = \cdots = Z_{i_1} \supsetneq Z_{i_1+1} = \cdots = Z_{i_2} \supsetneq \cdots = Z_{i_j} \supsetneq Z_{i_j+1} = \cdots = Z_k. \tag{2.4}$$

From Lemma 2.2, we have: $c_{Z_1}c_{Z_1Z_2}\cdots c_{Z_{k-1}Z_k}$ is equal to

$$c_{Z_1}q^{\dim(Z(Z_{i_1}))(i_1-1)}c_{Z_{i_1}Z_{i_2}}q^{\dim(Z(Z_{i_2}))(i_2-i_1-1)}\cdots c_{Z_{i_j}Z_k}q^{k-i_j-1}.$$

For $1 \le u \le j-1$, we have, $Z_{i_u} \supsetneq Z_{i_{u+1}}$. Thus, $Z_{i_u} \supsetneq Z_k$ for all $u:\ 1 \le u \le j$. Then by Lemma 2.6, we have $\dim(Z(Z_{i_u})) < \dim(Z(Z_k))$ for all $u:\ 1 \le u \le j$. Hence, for $1 \le u \le j$,

$$\dim(Z(Z_{i_u})) < m(n).$$

Therefore

$$\dim(Z(Z_{i_u})) \le m(n)-1$$

for $1 \le u \le j$. Hence, $c_{Z_1}c_{Z_1Z_2}\cdots c_{Z_{k-1}Z_k}$ is bounded above by

$$c_{Z_1}c_{Z_{i_1}Z_{i_2}}\cdots c_{Z_{i_j}Z_k}.q^{(m(n)-1)(i_j-j)}.q^{m(n)(k-i_j-1)},$$

which is bounded above by

$$c_{Z_1}c_{Z_{i_1}Z_{i_2}}\cdots c_{Z_{i_j}Z_k}.q^{(m(n)-1)(i_j)}.q^{m(n)(k-i_j)}.$$

Now, as each of $c_{Z_1}, c_{Z_{i_1}Z_{i_2}}, \ldots, c_{Z_{i_j}Z_k}$ cannot be more than q^{n^2}, we have,

$$\begin{aligned} c_{Z_1}c_{Z_1Z_2}\cdots c_{Z_{k-1}Z_k} &\leq q^{n^2(j+1)}.q^{[(m(n)-1)i_j+m(n)(k-i_j)]} \\ &= q^{n^2(j+1)}.q^{(m(n)k-i_j)} \end{aligned}$$

Here are some observations:

- We know that there are only a finite number of distinct algebras in $M_n(\mathbb{F}_q)$. Let that number be $f(n)$. For each j as $0 \leq j \leq n^2-1$, there cannot be more than $\binom{f(n)}{j+1}$ of them.
- Given $Z_1 \supseteq \cdots \supseteq Z_k$, in which $j+1$ of them are distinct, i.e., there is a strongly decreasing subsequence of $Z_1 \supseteq \cdots \supseteq Z_k$:

  $$Z_{i_1} \supsetneq Z_{i_2} \supsetneq \cdots \supsetneq Z_{i_j} \supsetneq Z_k,$$

  such that $Z_1 \supseteq \cdots \supseteq Z_k$, is as in Expression 2.4. Given this subset $S = \{i_1, \ldots, i_j\}$, at which the descents occur, $c_{Z_1}c_{Z_1Z_2}\cdots c_{Z_kZ_{k-1}}$ is bounded above by

  $$q^{n^2(j+1)}.q^{(m(n)k-\max(S))}.$$

  But then this S could be any size j subset of $\{1, \ldots, k-1\}$. So, $c(n,k,q)$ is bounded above by

  $$\sum_{j=0}^{n^2-1}\left(\binom{f(n)}{j+1}q^{n^2(j+1)}\sum_{\substack{S\subseteq\{1,\ldots,k-1\}\\|S|=j}}q^{(m(n)k-\max(S))}\right),$$

  which is equal to

  $$\sum_{j=0}^{n^2-1}\left(\binom{f(n)}{j+1}q^{n^2(j+1)}\sum_{r=j}^{k-1}\sum_{\substack{S\subseteq\{1,\ldots,k-1\}\\|S|=j\\\max(S)=r}}q^{(m(n)k-r)}\right).$$

  But this is equal to

  $$\sum_{j=0}^{n^2-1}\left(\binom{f(n)}{j+1}q^{n^2(j+1)}\sum_{r=j}^{k-1}\binom{r-1}{j-1}q^{(m(n)k-r)}\right).$$

  (Once r is chosen, the remaining $j-1$ numbers are chosen from $1, \ldots, r-1$ in $\binom{r-1}{j-1}$ ways.)

Now, as $\binom{r-1}{j-1} \le r^j$, we get that

$$\begin{aligned} c(n,k,q) &\le q^{m(n)k} \sum_{j=0}^{n^2-1} \left(\binom{f(n)}{j+1} q^{n^2(j+1)} \sum_{r=j}^{k-1} r^j q^{-r} \right) \\ &\le q^{m(n)k} \sum_{j=0}^{n^2-1} \left(\binom{f(n)}{j+1} q^{n^2(j+1)} \sum_{r=0}^{\infty} r^j q^{-r} \right) \end{aligned}$$

Now, for any fixed j, we can see by any of the routine tests (either the root or ratio test) that the series,

$$\sum_{r=0}^{\infty} r^j q^{-r}, \text{ converges.}$$

So, let

$$C_2 = \sum_{j=0}^{n^2-1} \left(\binom{f(n)}{j+1} q^{n^2(j+1)} \sum_{r=0}^{\infty} r^j q^{-r} \right),$$

then we have

$$c(n,k,q) \le s_2 q^{m(n)k}.$$

So we have found positive constants C_1 and C_2 such that

$$C_1 q^{m(n)k} \le c(n,k,q) \le C_2 q^{m(n)k}$$

Hence $c(n,k,q)$, as a function of k is asymptotically $q^{m(n)k}$ upto some constant factor.

3. Asymptotic of Counting Tuples of Commuting Matrices

In this section, instead of looking at simultaneous similarity classes of commuting tuples, we will look at the asymptotic of counting total number of tuples of commuting matrices. Let $C(n,k,q)$ denote the total number of k-tuples of commuting $n \times n$ matrices over $\mathbb{F}_q$ i.e., the size of $M_n(\mathbb{F}_q)^{(k)}$. Then we have,

$$C(n,k,q) = \sum_{Z \subseteq M_n(\mathbb{F}_q)} \frac{|GL_n(\mathbb{F}_q)|}{|Z^*|} C_Z, \tag{3.1}$$

where Z varies over conjugacy classes of subalgebras of $M_n(\mathbb{F}_q)$, Z^* is the group of units of Z, and C_Z is the total number of simultaneous similarity classes of k-tuples of commuting matrices whose common centralizer algebra is isomorphic to Z.

From the previous section, we see that

$$C_Z = \sum_{\substack{Z_1 \supseteq \cdots \supseteq Z_k \\ Z_k = Z}} c_{Z_1} c_{Z_1 Z_2} \cdots c_{Z_{k-1} Z_k},$$

where $Z_k = Z$. So we can rewrite equation (3.1) as

$$C(n,k,q) = \sum_{Z_1 \supseteq \cdots \supseteq Z_k} \frac{|GL_n(\mathbb{F}_q)|}{|Z_k^*|} c_{Z_1} c_{Z_1 Z_2} \cdots c_{Z_{k-1} Z_k}. \tag{3.2}$$

Equation 3.2 is a modified version of equation (2.2).

Now, if we consider tuples, $(A_1, \dots, A_k)$, whose first $l_0 (= \left[\frac{n}{2}\right] + 1)$ coordinates are as in examples 2.3 and 2.4, then we get $|Z_k| = q^{m(n)}$, and $|Z_k^*| = (q-1)q^{\left[\frac{n^2}{4}\right]}$. So we have

$$\frac{|GL_n(\mathbb{F}_q)|}{(q-1)q^{\left[\frac{n^2}{4}\right]}} c_{Z_1} c_{Z_1 Z_2} \cdots c_{Z_{l_0}} q^{m(n)(k-l_0)} \leq C(n,k,q)$$

Thus, choose

$$D_1 = \frac{|GL_n(\mathbb{F}_q)|}{(q-1)q^{\left[\frac{n^2}{4}\right]}} c_{Z_1} c_{Z_1 Z_2} \cdots c_{Z_{l_0}} q^{-m(n) l_0}.$$

Then we get $D_1 q^{m(n)k} \leq C(n,k,q)$.

Now we can find an upper bound for $C(n,k,q)$. From equation (3.2) we have $C(n,k,q)$ equal to

$$\sum_{Z_1 \supseteq \cdots \supseteq Z_k} \frac{|GL_n(\mathbb{F}_q)|}{|Z_k^*|} c_{Z_1} c_{Z_1 Z_2} \cdots c_{Z_{k-1} Z_k}.$$

Now, as $GL_n(\mathbb{F}_q)$ has only a finite number of subgroups, $\frac{|GL_n(\mathbb{F}_q)|}{|Z_k^*|}$ is bounded above. Let that bound be $G(q)$. So we have

$$\begin{aligned} C(n,k,q) &\leq G(q) \sum_{Z_1 \supseteq \cdots \supseteq Z_k} c_{Z_1} c_{Z_1 Z_2} \cdots c_{Z_{k-1} Z_k} \\ &= G(q) c(n,k,q) \\ &\leq G(q) C_2 q^{m(n)k} \text{ (From section 2)} \end{aligned}$$

So let $D_2 = G(q)C_2$, then we have $D_2 > 0$ such that, $C(n,k,q) \leq D_2 q^{m(n)k}$. This proves the theorem:

Theorem 3.1. *The total number of k-tuples of commuting $n \times n$ matrices over $\mathbb{F}_q$: $C(n,k,q)$ is asymptotic to $q^{m(n)k}$ as a function of k.*

Keeping n and q fixed, we could find the asymptotics of $c(n,k,q)$ and $C(n,k,q)$ as k goes to ∞. We could instead keep k and q fixed and ask what are the asymptotics of $c(n,k,q)$ and $C(n,k,q)$ as n goes to ∞. We could also keep k and n fixed and ask for the asymptotics of $c(n,k,q)$ and $C(n,k,q)$ as a function of q.

Acknowledgements. I thank my supervisor Prof. Amritanshu Prasad for the discussions we had about this topic and for feedback on the draft of this paper, and Prof. S. Viswanath for a few suggestions while giving a talk on the results of this paper.

References

[Ago14] A. L. Agore. Parabolic subalgebras of matrix algebras. eprint `http://arxiv.org/pdf/1403.0773.pdf`, 2014.

[Gir98] Frank Girth. Some asymptotics for triangular matrices over finite fields. *Linear Algebra and its Applications*, 282:249–261, 1998.

[Jac44] N. Jacobson. Schur's theorems on commutative matrices. *Bull. Amer. Math. Soc.*, 1944.

[NP95] P.M. Neumann and C.E. Praeger. Cyclic matrices over finite fields. *J. London Math. Soc.*, 52(2):263–284, 1995.

[Sha16] Uday Bhaskar Sharma. Simultaneous similairty classes of commuting matrices over a finite field. *Linear Algebra Appl.*, 501:48–97, 2016.

[Sto88] Richard Stong. Some asymptotic results on finite vector spaces. *Adv. App. Math*, 9:167–199, 1988.

The Institute of Mathematical Sciences, Chennai.
E-mail address: `udaybs@imsc.res.in`